МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет управления территориями
Кафедра землеустройства и кадастров

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 5387FD2AF5B17FED816FDE9A1D4973B1
Владелец: Степанченко Алексей Леонидович
Действителен: с 21.07.2025 по 14.10.2026

«УТВЕРЖДАЮ»
Проректор
А. Л. Степанченко
15 мая 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «Б1.В.ДВ.03.02 СИСТЕМЫ ХРАНЕНИЯ И ЗАЩИТЫ КАДАСТРОВОЙ ИНФОРМАЦИИ»

Уровень высшего образования: магистратура

Направление подготовки: 21.04.02 Землеустройство и кадастры

Направленность (профиль) подготовки: Управление недвижимостью и развитием территорий

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Год набора (приема на обучение): 2026

Срок получения образования: 2 года

Объем: в зачетных единицах: 2 з.е.
в академических часах: 72 ак.ч.

Москва, 2026

Разработчики:

Доцент кафедры Землеустройства и кадастров, к.н., доцент
Абросимов В. В.

Профессор кафедры Землеустройства и кадастров, д.н., доцент
Литвиненко М. В.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 21.04.02 Землеустройство и кадастры, утвержденного приказом Минобрнауки от 11.08.2020 № 945

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Управления территориями	Председатель ученого совета факультета	Воронцова А. А.	Рассмотрено	25.11.2025, № 8-2025

Содержание

1. Цель и задачи освоения дисциплины (модуля)

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

3. Место дисциплины в структуре ОП

4. Объем дисциплины и виды учебной работы

5. Содержание дисциплины
   5.1. Разделы, темы дисциплины и виды занятий
   5.2. Содержание разделов, тем дисциплины и формы текущего контроля

6. Оценочные материалы текущего контроля

7. Оценочные материалы промежуточной аттестации

8. Порядок проведения промежуточной аттестации

9. Материально-техническое и учебно-методическое обеспечение дисциплины
   9.1. Перечень основной и дополнительной учебной литературы
   9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся
   9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине
   9.4. Оборудование и технические средства обучения

10. Методические указания по освоению дисциплины (модуля)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - получение обучающимися теоретических знаний об актуальности вопроса защиты информации и об электронном документообороте, комплексной системе функционирования информационной безопасности и её нормативном обеспечении, об угрозах безопасности информации и её методах защиты с применением технологий защиты информации в профессиональной деятельности

Задачи изучения дисциплины:

- формирование понятий по существующим угрозам безопасности информации, подбору и применению современных методов и способов защиты информации;
- формирование умений применять полученные знания в практической деятельности, решать практические задачи организации защиты информации в коммерческих и государственных структурах Росреестра РФ;
- освоение навыков по защите информации в корпоративных вычислительных сетях и при работе в интернет.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ПК-3 Способность получать и обрабатывать информацию из различных источников в целях планирования и организации работ по определению кадастровой стоимости объектов недвижимости

ПК-3.1 Планирует деятельность структурного подразделения по вверенному направлению, организует работы по направлениям деятельности структурных подразделений

Знать:

ПК-3.1/Зн1 Принципы планирования и организации деятельности структурных подразделений в землеустроительной и кадастровой деятельности

Уметь:

ПК-3.1/Ум1 Планировать и распределять задачи среди сотрудников отдела

Владеть:

ПК-3.1/Нв1 Навыком эффективного управления работами подразделения, направленного на достижение поставленных целей и задач

ПК-3.2 Обеспечивает внедрение информационно-аналитических, правовых систем и баз данных для определения кадастровой стоимости объектов недвижимости, определяет потребности в ресурсах, обеспечивающих деятельность структурного подразделения по вверенному направлению, готовит предложения для совершенствования методических материалов по определению кадастровой стоимости объектов недвижимости

Знать:

ПК-3.2/Зн1 Принципы работы информационно-аналитических и правовых систем, используемых для определения кадастровой стоимости недвижимости

Уметь:

ПК-3.2/Ум1 Оценивать потребности подразделения в ресурсах для выполнения задач по определению кадастровой стоимости

Владеть:

ПК-3.2/Нв1 Навыком подготовки предложений по совершенствованию методических материалов и подходов к оценке кадастровой стоимости объектов недвижимости

ПК-5 Способность использовать средства автоматизации при работе с автоматизированной информационной системой ФГИС ЕГРН

ПК-5.1 Готовит предложения по развитию и модернизации программно-аппаратного комплекса Единого государственного реестра прав на недвижимое имущество и ГКН, внедряет новые программные средства в сфере государственного кадастрового учета

Знать:

ПК-5.1/Зн1 Принципы работы и требования к программно-аппаратному комплексу Единого государственного реестра недвижимости

Уметь:

ПК-5.1/Ум1 Анализировать существующий комплекс и предлагать решения по его развитию и модернизации

Владеть:

ПК-5.1/Нв1 Навыком внедрения новых программных средств и технологий в процессы государственного кадастрового учета

ПК-5.2 Формирует предложения по оснащению подразделения программно-техническими средствами, необходимыми для эксплуатации информационных систем, изучает и анализирует методы и технологии ведения ГКН, подбор и подготовку методических материалов, касающихся новых технологий ведения ГКН, реализует мероприятия по защите информации с применением программных средств

Знать:

ПК-5.2/Зн1 Требования к программно-техническому оснащению подразделения для эксплуатации информационных систем

Уметь:

ПК-5.2/Ум1 Изучать и анализировать новые методы и технологии ведения кадастра недвижимости

Владеть:

ПК-5.2/Нв1 Навыком подбора и подготовки методических материалов по новым технологиям ведения кадастра, а также реализации мероприятий по защите информации с использованием программных средств

ПК-6 Способность использовать средства автоматизации и программно-вычислительные комплексы при статистической обработке информации, математическом и компьютерном моделировании схем и проектов землеустройства и формировании информационных баз данных

ПК-6.1 Проводит эксперименты, наблюдения и измерения в области землеустройства, разрабатывает специальные программы компьютерной разработки проектов землеустройства

Знать:

ПК-6.1/Зн1 Методы и технологии проведения экспериментов, наблюдений и измерений в землеустроительной деятельности

Уметь:

ПК-6.1/Ум1 Разрабатывать специальные программы и использовать компьютерные технологии для создания проектов землеустройства

Владеть:

ПК-6.1/Нв1 Навыком применения программных средств для проектирования и разработки землеустроительных проектов

ПК-6.2 Создаёт математические модели и системы сбора, обработки и анализа информации в области землеустройства, мониторинга, земельного контроля (надзора), кадастров, проводит компьютерное моделирование схем и проектов землеустройства, в том числе трехмерных моделей, формирует технологическую и отчетную документацию по результатам работ

Знать:

ПК-6.2/Зн1 Методы математического моделирования и компьютерного проектирования в землеустроительной деятельности

Уметь:

ПК-6.2/Ум1 Создавать и применять математические модели для сбора, обработки и анализа информации

Владеть:

ПК-6.2/Нв1 Навыком компьютерного моделирования проектов, включая трёхмерные модели, и оформления итоговой технологической и отчётной документации

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.В.ДВ.03.02 «Системы хранения и защиты кадастровой информации» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 3.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
3 семестр	72	2	17	17	38	Зачет
Всего	72	2	17	17	38	

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	его	кционные занятия	актические занятия	мостоятельная работа	анируемые результаты чения, соотнесенные с ультатами освоения ограммы

	Все	Лек	Пр	Сам	Пла обу рез прс
Раздел 1. Актуальность вопроса защиты информации.	**14**	**4**	**4**	**6**	ПК-3.1 ПК-3.2
Тема 1.1. Информационная безопасность.	1	1			
Тема 1.2. Правовая основа.	4	1	1	2	
Тема 1.3. Наиболее значимые требования к системе построения защиты информации организации.	4	1	1	2	
Тема 1.4. Примерная схема разработки технических средств и методов создания СЗИ	5	1	2	2	
Раздел 2. Электронный документооборот.	**12**	**3**	**3**	**6**	ПК-3.1 ПК-3.2
Тема 2.1. Регулирование отношений, связанных с защитой информации.	4	1	1	2	
Тема 2.2. ЭЦП, как вариант защиты электронного документооборота.	4	1	1	2	
Тема 2.3. Обеспечение непрерывности бизнеса.	4	1	1	2	
Раздел 3. Комплексная система обеспечения информационной безопасности.	**25**	**6,5**	**4,5**	**14**	ПК-3.1 ПК-3.2 ПК-5.1 ПК-5.2 ПК-6.1 ПК-6.2
Тема 3.1. Проектирование системы защиты информации объекта.	3,5	1	0,5	2	
Тема 3.2. Критерии построения комплексной системы обеспечения информационной безопасности.	3,5	1	0,5	2	
Тема 3.3. Комплекс мероприятий для обеспечения защиты информации.	3,5	1	0,5	2	
Тема 3.4. Меры по предотвращению и защите от информационных атак конкурентов.	3,5	1	0,5	2	
Тема 3.5. Важность защиты корпоративных сетей.	3,5	1	0,5	2	
Тема 3.6. Подбор персонала.	4	1	1	2	
Тема 3.7. Разработка комплекса мероприятий для организации деловой (оперативной) разведки в интересах коммерческой фирмы.	3,5	0,5	1	2	
Раздел 4. Нормативное обеспечение информационной безопасности.	**10**	**1,5**	**2,5**	**6**	ПК-3.1 ПК-3.2 ПК-5.1

Тема 4.1. Ответственность за нарушение законодательства Российской Федерации в области персональных данных. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».	3,5	0,5	1	2	ПК-5.2 ПК-6.1 ПК-6.2
Тема 4.2. Законодательство в области персональных данных.	3,5	0,5	1	2	
Тема 4.3. Ответственность за разглашение сведений, составляющих государственную тайну.	3	0,5	0,5	2	
Раздел 5. Угрозы безопасности информации.	**11**	**2**	**3**	**6**	ПК-6.2
Тема 5.1. Угрозы безопасности информации, обрабатываемой на ПЭВМ.	3,5	0,5	1	2	
Тема 5.2. Угрозы безопасности информации.	3,5	0,5	1	2	
Тема 5.3. Несанкционированный доступ к сетям и сетевым ресурсам.	4	1	1	2	
Итого	**72**	**17**	**17**	**38**	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Актуальность вопроса защиты информации.

Тема 1.1. Информационная безопасность.

Стратегия информационной безопасности. Глобальность и разнородность современных корпоративных сетей. Интегрированная система охраны объектов. Некоторые аспекты защиты графической информации. Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера.

Тема 1.2. Правовая основа.

Федеральный Закон "Об информации, информатизации и защите информации" номер 1-ФЗ. Лицензирование отдельных видов деятельности. Преступления в сфере компьютерной информации. Основные виды частной и охранной деятельности. Юридическая сила «электронного документа». Использование электронных цифровых подписей.

Тема 1.3. Наиболее значимые требования к системе построения защиты информации организации.

Формирование политики информационной безопасности. Роль организационных мероприятий: действия в области управления персоналом, реакция на нарушения режима безопасности, планирование восстановительных работ. ISO 17799 - стандарт, содержащий каталог лучших практик обеспечения информационной безопасности. Внутренний или внешний аудит информационной безопасности кадастровой компании.

Тема 1.4. Примерная схема разработки технических средств и методов создания СЗИ

Защита от внешнего и внутреннего несанкционированного доступа. Обеспечение целостности данных на логическом и физическом уровнях. Защита носителей. Защита инфраструктуры. Защита от случайных потерь. Экономические аспекты. Разработка аппаратно-программных средств.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 2. Электронный документооборот.

Тема 2.1. Регулирование отношений, связанных с защитой информации.

Цель проведения защитных мер на объекте. Защищаемые объекты информатизации. Организационные меры. Испытанный метод защиты информации от НСД – шифрование. Необходимость обеспечения не только конфиденциальности, но и целостности сообщения.

Тема 2.2. ЭЦП, как вариант защиты электронного документооборота.

Понятие принципа ЭЦП (электронной цифровой подписи). Подпись документов при помощи симметричных криптосистем. Подпись документов при помощи криптосистем с открытыми ключами. Хэш-функция. Хранение, распределение ключей. Требования пользователей. Атаки на цифровую подпись. Авторизация. Идентификация. Аутентификация.

Тема 2.3. Обеспечение непрерывности бизнеса.

Планирование непрерывности деятельности. План действий в нештатной ситуации. Хорошо обученные и тренированные "аварийные группы".

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 3. Комплексная система обеспечения информационной безопасности.

Тема 3.1. Проектирование системы защиты информации объекта.

Интегрированная система безопасности (ИСБ). Определение требований к системе защиты информации. Определение и подготовка лиц, ответственных за обеспечение безопасности информации. Установление мер контроля и ответственности за соблюдение всех правил защиты информации.

Тема 3.2. Критерии построения комплексной системы обеспечения информационной безопасности.

Подсистема управления доступом. Подсистема регистрации и учета. Криптографическая подсистема. Подсистема обеспечения целостности.

Текущий контроль

Вид (форма) контроля

Расчетно-графическая работа

Тема 3.3. Комплекс мероприятий для обеспечения защиты информации.

Административные меры. Резервное копирование. Разграничение доступа. Регистрация действий пользователей. Защита информации при передаче ее по каналам связи (шифрование). Маркирование документов. Закрытое обсуждение. Использование соглашения о конфиденциальности. Ограничение доступа к информации. Информирование.

Текущий контроль

Вид (форма) контроля
Расчетно-графическая работа

Тема 3.4. Меры по предотвращению и защите от информационных атак конкурентов.

Классифицирование по возможным каналам утечки. Виды специальных проверок. Комплекс мероприятий для предотвращения НСД и защиты информации. Присвоение конфиденциальной информации грифа «Для служебного пользования».

Текущий контроль

Вид (форма) контроля
Расчетно-графическая работа

Тема 3.5. Важность защиты корпоративных сетей.

Основные способы проникновения вредоносных программ в сеть к сетевым ресурсам. Основные требования к защите сетей, объектов информации от вредоносных программ. Защита корпоративной сети кадастровой организации от вторжения извне, если она подключена к Internet. Исключение возможности утечки (хищения) большого объема данных. Обеспечение своевременного обнаружения единичной и систематической утечки (хищения) информации. Защита информации от сброса на различные носители посторонними лицами и нечестными сотрудниками фирмы. Запрет пользования мобильными телефонами на рабочих местах и выход в интернет в рабочее время.

Текущий контроль

Вид (форма) контроля
Расчетно-графическая работа

Тема 3.6. Подбор персонала.

Принципы планирования персонала. Группы критериев кадровой безопасности. Эффективный подбор персонала. Первичный отбор. Собеседование. «Испытания». Профессиональные тесты, собеседование с экспертами. Психологическое тестирование. Корпоративная культура.

Текущий контроль

Вид (форма) контроля
Расчетно-графическая работа

Тема 3.7. Разработка комплекса мероприятий для организации деловой (оперативной) разведки в интересах коммерческой фирмы.

Основные правила развития системы обеспечения подразделения информацией о конкурентах. Мероприятия, необходимые для организации деловой разведки в интересах фирмы. Создание интегрированного банка данных. Налаживание постоянной циркуляции информации от отдела деловой разведки к ее потребителям в лице других отделов кадастровой организации.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 4. Нормативное обеспечение информационной безопасности.

Тема 4.1. Ответственность за нарушение законодательства Российской Федерации в области персональных данных.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Права субъекта персональных данных. Обязанности оператора при сборе персональных данных. Контроль и надзор за обработкой персональных данных. Законодательство в области персональных данных.

Текущий контроль

Вид (форма) контроля
Расчетно-графическая работа

Тема 4.2. Законодательство в области персональных данных.

Конституция Российской Федерации, Федеральные Законы, Кодексы Российской Федерации.

Текущий контроль

Вид (форма) контроля
Расчетно-графическая работа

Тема 4.3. Ответственность за разглашение сведений, составляющих государственную тайну.

Российская Федерация «Закон о государственной тайне». Перечень сведений, составляющих государственную тайну. Принципы отнесения сведений к государственной тайне. Органы защиты государственной тайны. Контроль за обеспечением защиты государственной тайны. Сведения, отнесенные к государственной тайне.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 5. Угрозы безопасности информации.

Тема 5.1. Угрозы безопасности информации, обрабатываемой на ПЭВМ.

Цели защиты информации, перечень необходимых мер, обеспечивающих эту защиту. Случайные и умышленные угрозы. Разграничение полномочий пользователей. Компьютерные вирусы. Повышения квалификации обслуживающего персонала и пользователей.

Тема 5.2. Угрозы безопасности информации.

Проблемы информационной безопасности. Действия хакеров. Некоторые методы действия хакеров.

Тема 5.3. Несанкционированный доступ к сетям и сетевым ресурсам.

Уязвимые места в компьютерных сетях. Требования к паролям. Интерактивные последовательности «вопрос − ответ».

Текущий контроль

Вид (форма) контроля
Тестирование

6. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Зачет, 3 семестр.

Промежуточная аттестация проводится в форме тестирования в системе дистанционного обучения https://lms.miigaik.ru/. Зачет по дисциплине выставляется при условии, что итоговый тест пройден обучающимся на оценку не ниже «удовлетворительно», и контрольная работа зачтена.

Порядок выставления оценок за итоговый тест:

Итоговый тест состоит из 10 вопросов.

Оценка рассчитывается следующим образом:

9-10 правильных ответов - "отлично"

7-8 правильных ответов - "хорошо"

5-6 правильных ответов - "удовлетворительно"

0-4 правильных ответов - "неудовлетворительно"

Дается 3 попытки выполнения теста.

Разрешено попыток: 3

Ограничение по времени: 20 мин.

Критерии выставления отметки «зачтено» за контрольную работу приведены в методических рекомендациях по выполнению контрольной работы.

7. Оценочные материалы текущего контроля

Раздел 1. Актуальность вопроса защиты информации.
Контролируемые ИДК: ПК-3.1 ПК-3.2

Тема 1.4. Примерная схема разработки технических средств и методов создания СЗИ

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой из следующих нормативных документов рассматривает вопросы предотвращения несанкционированных действий по копированию информации?

1.ФЗ "Об информации, информатизации и защите информации"
2.ФЗ "Об электронной цифровой подписи"

2. В каких из следующих случаев информация составляет служебную или коммерческую тайну?

1.Информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам
2.К информации нет свободного доступа на законном основании
3.Обладатель информации принимает меры к охране ее конфиденциальности
4.Информация создана посредством шифровальных (криптографических) средств

3. Какой из перечисленных уровней безопасности используется для защиты интересов субъектов информационных отношений?

1.Экономический
2.Социальный
3. Административный

4. В структуру информационной безопасности организации входят:

1.Требования
2.Стандарты
3.Организационно-распорядительные и нормативно-технические документы
4.Уровенный доступ к получению информации

5. Какие государственные органы организуют систему лицензирования?

1.Гостехкомиссия
2.ФСБ
3.Министерство юстиции
4.Комиссия по регулированию информационных отношений

6. Какие из перечисленных видов деятельности нельзя осуществлять без лицензии?

1.Регистрация владельцев электронных цифровых подписей
2.Техническая защита конфиденциальной информации
3.Выявление юридическими лицами и предпринимателями, устройств, негласно получающих информацию, для обеспечения защиты своих собственных интересов

7. Какой из следующих нормативных документов рассматривает вопросы обеспечения прав субъектов при производстве и применении информационных систем?

1.ФЗ "Об информации, информатизации и защите информации"
2.ФЗ "Об электронной цифровой подписи"
3.ФЗ "О лицензировании отдельных видов деятельности"

Раздел 2. Электронный документооборот.

Контролируемые ИДК: ПК-3.1 ПК-3.2

Тема 2.3. Обеспечение непрерывности бизнеса.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Верно ли утверждение: согласно требованиям предъявляемым к алгоритмам шифрования, защищенность информации основывается на знании ключа и зависит от того, известен алгоритм шифрования или нет

1.Да
2.Нет

2. Статистическое кодирование иначе называется...

1.архивацией
2.криптоанализом
3.энтропией

3. Процесс подтверждения идентифицированным объектом своего уровня доступа и «уверенность» системы в том, что идентифицированный объект действительно тот, за кого себя выдает называется...

1. Аутентификация
2. Идентификация
3. Нет верных ответов

4. Ограниченный срок действия имеет...

1. Цифровая подпись
2. Цифровой сертификат
3. Эталонная копия

5. Каким стандартам должна удовлетворять цифровая подпись?

1. Она должна подтверждать, что подписывающее лицо не случайно подписало электронный документ
2. Она должна подтверждать, что только подписывающее лицо, и только оно, подписало электронный документ
3. Она должна зависеть от содержания подписываемого документа
4. Она не должна зависеть от времени подписания документа
5. Подписывающее лицо должно иметь возможность впоследствии отказаться от факта подписи документа

Раздел 3. Комплексная система обеспечения информационной безопасности.

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-5.1 ПК-5.2 ПК-6.1 ПК-6.2

Тема 3.2. Критерии построения комплексной системы обеспечения информационной безопасности.

Форма контроля/оценочное средство: Расчетно-графическая работа

Вопросы/Задания:

1. Раскрыть понятия: информации, компьютерной информации (формы существования компьютерной информации)

2. Информационная безопасность. Основные компоненты концептуальной модели информационной безопасности

3. Информация как собственность. Собственник, владелец и пользователь информационных ресурсов

4. Угроза информации в нарушении ее целостности

Тема 3.3. Комплекс мероприятий для обеспечения защиты информации.

Форма контроля/оценочное средство: Расчетно-графическая работа

Вопросы/Задания:

1. Угроза информации в нарушении ее конфиденциальности

2. Угроза информации в нарушении ее доступности

3. Неправомерные способы овладения информацией. Разглашение. Утечка. Несанкционированный доступ

4. Основные способы, средства и направления защиты компьютерной информации

Тема 3.4. Меры по предотвращению и защите от информационных атак конкурентов.

Форма контроля/оценочное средство: Расчетно-графическая работа

Вопросы/Задания:

1. Требования к системе защиты информации

2. Модель информационного нарушителя. Цели информационных нарушителей. Иерархия информационных нарушителей

3. Хакеры. Классификации хакеров

4. Определение и классификация правовой защиты информации

5. Интересы личности, общества и государства в информационной сфере

Тема 3.5. Важность защиты корпоративных сетей.

Форма контроля/оценочное средство: Расчетно-графическая работа

Вопросы/Задания:

1. Информация как собственность. Собственник, владелец и пользователь информационных ресурсов

2. Структура информационных ресурсов по характеру доступа

3. Понятие и содержание государственной тайны. Закон РФ «О Государственной тайне»

4. Электронная цифровая подпись. Закон об электронной цифровой подписи

5. Сфера действия и основные понятия федерального закона «Об информации, информатизации и защите информации»

Тема 3.6. Подбор персонала.

Форма контроля/оценочное средство: Расчетно-графическая работа

Вопросы/Задания:

1. Проблема целостности и проблема конфиденциальности информации на магнитных носителях

2. Понятие и классификация криптографических методов и средств защиты информации

3. Аутентификация электронных документов и сообщений. Системы электронно-цифровой подписи

4. Определение вредоносной программы. Происхождение вирусов. Отличительные свойства компьютерных вирусов. Сущность вирусного заражения

Тема 3.7. Разработка комплекса мероприятий для организации деловой (оперативной) разведки в интересах коммерческой фирмы.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какая из перечисленных подсистем защиты информации отвечает за управление потоками информации?

1. Подсистема управления доступом
2. Подсистема регистрации и учета
3. Криптографическая подсистема
4. Подсистема обеспечения целостности

2. Какие из перечисленных операций выполняет криптографическая подсистема?

1.Шифрование конфиденциальной информации

2.Использование аттестованных криптографических средств
3.Физическая охрана средств вычислительной техники и носителей информации
4.Тестирование системы защиты информации
5.Наличие службы защиты информации

3. Продолжите предложение. Бумажные и электронные документы, содержащие конфиденциальную информацию, подлежат обязательному маркированию путем проставления грифа конфиденциальности...

1. В правом верхнем углу титульного листа
2. В правом нижнем углу титульного листа
3. После подписи ответственного лица
4. Перед подписью ответственного лица

4. Какие из следующих критериев характеризуют кадровую безопасность?

1.Показатели численного состава персонала и его динамики
2. Показатели квалификации и интеллектуального потенциала
3. Показатели эффективности использования персонала
4. Показатели качества мотивационной системы
5.Показатели сверхурочной работы персонала

5. Какой из перечисленных видов несанкционированного получения информации является основным в топографо-геодезической деятельности?

1.Прослушивание телефонных каналов связи
2.Визуальное наблюдение за объектом
3.Перехват компьютерной информации

Раздел 4. Нормативное обеспечение информационной безопасности.

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-5.1 ПК-5.2 ПК-6.1 ПК-6.2

Тема 4.1. Ответственность за нарушение законодательства Российской Федерации в области персональных данных.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Форма контроля/оценочное средство: Расчетно-графическая работа

Вопросы/Задания:

1. Антивирусное программное обеспечение. Антивирусная профилактика

2. Основные этапы обеспечения информационной безопасности в компьютерной системе

3. Модели разграничения доступа в компьютерных системах

Тема 4.2. Законодательство в области персональных данных.

Форма контроля/оценочное средство: Расчетно-графическая работа

Вопросы/Задания:

1. Характеристики средств защиты информации, создаваемые аппаратно-программными средствами. Функции СЗИ. Схема защиты информации

2. Блокирование доступа злоумышленника к закрытым, виртуальным дискам, содержащим конфиденциальные данные и программы их обработки. Способы аутентификации личности

3. Политика межсетевого взаимодействия. Политика сетевой безопасности

4. Парольная система аутентификации личности пользователя. Пароль пользователя. Вероятность подбора пароля. Атаки на парольную систему. Требования к парольной системе. Минимальная длина пароля. Издержки «человеческого фактора». Рекомендации по выбору паролей

Тема 4.3. Ответственность за разглашение сведений, составляющих государственную тайну.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой вид наказания для юридических лиц в соответствии с Кодексом об административных правонарушениях РФ влечет нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)?

1.Ответственность не предусмотрена
2.Отстранение от должности руководителя организации
3.Предупреждение или наложение административного штрафа

2. Какой вид ответственности предусмотрен за неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина?

1.Административная, уголовная
2.Гражданская, дисциплинарная
3.Гражданская, административная

3. Предусмотрена ли за нарушение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных« уголовная и административная ответственность?

1.Только административная
2. Нет
3. Да

4. Понятие грифа секретности обозначает...

1. Специальные отметки на сопроводительном письме к документу
2. Реквизиты, свидетельствующие о закрытости документа
3. Реквизиты, свидетельствующие о степени секретности сведений

5. Какая ответственность предусмотрена за утрату документов, содержащих государственную тайну (за нарушения, которые повлекли по неосторожности утрату таких документов и наступление тяжких последствий)?

1. Объявление неполного служебного соответствия
2. Ограничение свободы, либо арест, либо лишение свободы с лишением права занимать определенные должности
3. Объявление строгого выговора

Раздел 5. Угрозы безопасности информации.

Контролируемые ИДК: ПК-6.2

Тема 5.3. Несанкционированный доступ к сетям и сетевым ресурсам.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Существование информации в неискаженном виде называется...

1. Доступностью информации
2.Целостностью информации
3.Конфиденциальностью информации
4. Нет верных ответов

2. Какие из следующих примеров являются случайными угрозами сохранности информации?

1. Потеря информации, связанная с неправильным хранением архивных данных
2. Сбой кабельной системы
3. Потеря данных при заражении системы компьютерными вирусами
4. Перехват компьютерной информации
5. Контроль и прослушивание телефонных каналов связи

3. Если пользователь входит в систему в первый раз, как правило, применяется...

1. Одноразовый код

2. Двоичный код
3. Интерактивная последовательность ‘вопрос ? ответ’
4. Ключевая фраза
5. Нет верных ответов

4. Свойство информации, указывающее на необходимость введения ограничений на доступ к данной информации это...

1.Ограниченность информации
2. Конфиденциальность информации
3. Целостность информации
4. Доступность информации

5. Верно ли утверждение: несанкционированный доступ к информации и сетевым ресурсам является случайной угрозой безопасности и сохранности информации.

1. Да
2. Нет

8. Оценочные материалы промежуточной аттестации

3 семестр, Зачет

Контролируемые ИДК: ПК-3.1 ПК-5.1 ПК-6.1 ПК-3.2 ПК-5.2 ПК-6.2

Вопросы/Задания:

1. Для какого из перечисленных видов деятельности нет необходимости в лицензии?

1.Выдача сертификатов ключей электронных цифровых подписей;
2.Регистрация владельцев электронных цифровых подписей;
3.Выявление юридическими лицами и предпринимателями, устройств, негласно получающих информацию, для обеспечения защиты своих собственных интересов;
4.Техническая защита конфиденциальной информации;
5.Приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, предпринимателями и юридическими лицами

2. Что из перечисленного относится к защищаемым объектам информатизации?

1.Вычислительная техника;
2.Переговорные и телевизионные устройства;
3.Операционные системы;
4.Помещения, используемые для ведения закрытых переговоров;
5.Сотрудники работающие в операционных системах и с вычислительной техникой;
6.Нормативно-техническая документация

3. Какая из следующих подсистем защиты информации отвечает за учет носителей информации?

1. Подсистема управления доступом;
2. Подсистема регистрации и учета;
3. Криптографическая подсистема

4. Какие из следующих случаев можно отнести к случайным угрозам безопасности и сохранности информации?

1.Сбои систем архивации данных;
2.Потеря информации при заражении системы компьютерными вирусами;
3.Потеря информации, связанная с неправильным хранением архивных данных;
4.Фальсификация сообщений, отказ от факта получения информации или изменение времени ее приема;
5.Раскрытие и модификация данных и программ

5. Какую ответственность несут должностные лица и граждане, виновные в нарушении законодательства Российской Федерации о государственной тайне?

1.Финансовую ответственность в соответствии с действующим законодательством;

2.Уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством;
3.Не несут никакой ответственности

6. Как называется Федеральный Закон от 27 июля 2006 г. N 149-ФЗ, рассматривающий вопросы предотвращения несанкционированных действий по копированию информации?

7. Какой из уровней безопасности формирует правовые нормы в области информационных отношений?

8. Какой государственный орган организует систему лицензирования в сфере защиты информации?

9. На какой из стадий создания системы защиты информации выполняется обследование объекта информатизации?
1.Предпроектная стадия;
2.Стадия разработки проектов;
3.Стадия ввода в действие СЗИ

10. Статистическое кодирование иначе называется...

11. Хранение секретного ключа электронной цифровой подписи на жестком диске, может служить примером атаки на...

12. При электронно-цифровой защите информации ограниченный срок действия имеет...

13. Примером двухфакторной аутентификации является...

14. Архивация данных это...
1.Статистическое кодирование информации;
2.Дешифрирование информации;
3.Определение количества информации, приходящееся на один символ

15. Процесс подтверждения идентифицированным объектом своего уровня доступа и «уверенность» системы в том, что идентифицированный объект действительно тот, за кого себя выдает называется...
1.Аутентификация;
2.Идентификация;
3.Нет верных ответов

16. Каким требованиям должна удовлетворять цифровая подпись?
1.Цифровая подпись должна подтверждать, что подписывающее лицо не случайно подписало электронный документ;
2.Цифровая подпись должна подтверждать, что только подписывающее лицо, и только оно, подписало электронный документ;
3.Цифровая подпись не должна зависеть от содержания подписываемого документа и времени его подписания;
4.Подписывающее лицо не должно иметь возможности впоследствии отказаться от факта подписи документа

17. Процесс предотвращения негативных воздействий на безопасность предприятия за счет рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом называется...

18. Уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных является…

19. Реквизиты, свидетельствующие о степени секретности сведений, означают...

20. Какие из следующих примеров являются случайными угрозами сохранности информации?

1. Потеря информации, связанная с неправильным хранением архивных данных;
2. Сбой кабельной системы;
3. Потеря данных при заражении системы компьютерными вирусами;
4. Перехват компьютерной информации;
5. Контроль и прослушивание телефонных каналов связи;

21. Какой из следующих видов защиты компьютерной информации является самым распространенным?

1.Контроль доступа с помощью предметов, принадлежащих пользователю;
2.Контроль доступа, основанный на личностных характеристиках пользователя;
3.Контроль доступа, основанный на обладании специфической информацией

22. Кто из перечисленных лиц занимается обеспечением безопасности в фирме?

23. Какой из перечисленных видов несанкционированного получения информации является основным в топографо-геодезической деятельности?

24. Сложный комплекс предположений, бездоказательно принимаемых всеми членами конкретной организации и задающие общие рамки поведения, принимаемые большей частью организации называется...

25. Процесс изучения выдвигаемых кандидатов с целью определения их пригодности для выполнения функциональных обязанностей на определенной должности, называется...

26. В каком углу титульного листа бумажные и электронные документы, содержащие конфиденциальную информацию, подлежат обязательному маркированию путем проставления грифа конфиденциальности?

27. Какие из перечисленных операций выполняет криптографическая подсистема?

1.Шифрование конфиденциальной информации;
2.Использование аттестованных криптографических средств;
3.Физическая охрана средств вычислительной техники и носителей информации;
4.Тестирование системы защиты информации;
5.Наличие службы защиты информации

28. Какие из перечисленных операций выполняет подсистема обеспечения целостности?

1.Шифрование конфиденциальной информации;
2.Использование аттестованных криптографических средств;
3.Физическая охрана средств вычислительной техники и носителей информации;
4.Тестирование системы защиты информации;
5.Наличие службы защиты информации

29. Установите последовательность этапов процесса подбора кадров в кадастровой организации

•Сбор информации о возможных кандидатах;
•Принятие решения о назначения работника на должность;
•Сравнение характеристик кандидатов на одну должность и выбор более подходящего по качествам работника;
•Сопоставление совокупности качеств кандидатов и предъявляемых к ним требований;
•Проверку выполнения работником возложенных на него функций

30. Какие виды наказаний для должностных лиц в соответствии с Кодексом об административных правонарушениях РФ влечет нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)?

31. Для обработка персональных данных требуется согласие...

32. Существование информации в неискаженном виде называется...

33. Что влечет за собой разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей?

34. К какому виду ответственности уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) имеет право привлекать лиц, виновных в нарушении Федерального закона от 27.07.2006 № 152-ФЗ О персональных данных?

35. Защищаемые государством сведения, распространение которых может нанести ущерб безопасности России, обозначает понятие...

36. Понятие грифа секретности обозначает...

1.Специальные отметки на сопроводительном письме к документу
2.Реквизиты, свидетельствующие о закрытости документа
3.Реквизиты, свидетельствующие о степени секретности сведений

37. Каким Перечнем сведений, подлежащих засекречиванию надо руководствоваться при определении грифа секретности сведений, образующихся в деятельности Росреестра?

1.Перечнем сведений, подлежащих засекречиванию, Минобороны России
2.Перечнем сведений, подлежащих засекречиванию, Минюста России
3.Перечнем сведений, подлежащих засекречиванию, Минэкономразвития России

38. Какие из следующих примеров относятся к умышленным угрозам сохранности информации?

1.Несанкционированный доступ к информации и сетевым ресурсам;
2.Раскрытие, модификация или подмена трафика вычислительной сети;
3.Фальсификация сообщений, отказ от факта получения информации или изменение времени ее приема;
4.Потеря при заражении системы компьютерными вирусами;
5.Сбои кабельной системы

39. Какие виды контроля доступа применяются для защиты компьютерных сетей и отдельных компьютеров от несанкционированного использования?

1. Контроль с помощью предметов, принадлежащих пользователю;
2. Контроль основанный на личностных характеристиках пользователя;
3. Контроль основанный на обладании специфической информацией

40. Как называется свойство информации, указывающее на необходимость введения ограничений на доступ к данной информации определенному кругу пользователей?

1.Конфиденциальность;
2.Доступность;
3.Целостность;
4.Ограниченность

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Информационная безопасность и правовые основы защиты персональных данных: учебное пособие / А. В. Терехов, В. Н. Чернышов, А. В. Платенкин, А. В. Селезнев. - Информационная безопасность и правовые основы защиты персональных данных - Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2023. - 80 с. - 978-5-8265-2648-4. - Текст: электронный // IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/141049.html - Режим доступа: по подписке

Дополнительная литература

1. Горюхина Е. Ю. Информационная безопасность: учебное пособие / Е. Ю. Горюхина, Л. И. Литвинова, Н. В. Ткачева. - Информационная безопасность - Воронеж: Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2015. - 221 с. - 2227-8397. - Текст: электронный // IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/72672.html - Режим доступа: по подписке

9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. https://www.garant.ru - Информационно-правовой портал "Гарант"

Ресурсы «Интернет»

1. https://lms.miigaik.ru - Система дистанционного обучения МИИГАиК

9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

Не используется.

Перечень информационно-справочных систем
(обновление выполняется еженедельно)

Не используется.

9.4. Оборудование и технические средства обучения

Компьютерный класс

Интерактивная панель - 1 шт.

10. Методические указания по освоению дисциплины (модуля)

Освоение обучающимся учебной дисциплины «Системы хранения и защиты кадастровой информации» предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций и практических занятий. Самостоятельная работа включает выполнение одной контрольной работы.

Общий порядок выполнения контрольной работы:

- изучите методические указания по выполнению контрольной работы, размещенные в https://lms.miigaik.ru;

- выполните задания, результат сохраните в виде файла в формате pdf и отправьте на проверку преподавателю средствами https://lms.miigaik.ru ;
- результат выполнения контрольной работы оценивается по шкале "допущена к защите / допущена к защите с исправлениями / не допущена к защите". В случае, если контрольная работа допущена к защите без исправлений, студент приносит работу на очные занятия в распечатанном виде для защиты. В случае, если контрольная работа допущена к защите с исправлениями, студент, сделав исправления в работе, где это указано преподавателем, не присылает повторно работу на проверку, а приносит исправленную работу на очные занятия в распечатанном виде для защиты. В случае, если контрольная работа не допущена к защите, студент, сделав исправления в работе, где это указано преподавателем, присылает работу на проверку повторно, до тех пор, пока работа не будет допущена к защите без исправлений или с незначительными исправлениями.
Студенты, не защитившие результаты выполнения контрольной работы на положительную отметку, к промежуточной аттестации по дисциплине не допускаются.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.